ABSTRACT

This invention concerns a set of particular keys designed top rove the authenticity of an entity or the integrity of a message. The proof is established by a set of keys comprising: m(1) pairs of private Q_I and public $G_I=g_i^{2,}$ values; a public module n consisting of the product of f(2) prime factors; an exponent $v=2^k(k>1)$, linked by relationships of the type: $G_i.Q_i^v$ 1. mod n or G_i Q_I^v mod n. The set of keys is produced such that: among the m numbers obtained by increasing Q_I or its inverse modulo n to modulo n square, k-1 times rank, at least one of them is different from g_i; among the 2m equations: x^2 g_i mod n, x^2 $-g_i$ mod n at least one of them has solutions in x in the ring of the modulo n integers.